Sub a1

1. A method for securing the integrity of files prior to archiving of said files, involving an exchange between a client and a Time Source Provider (a trusted third party) said method comprising the steps of:

the client generating a Public and a Private Key pair;

the client generating attributes of the to be archived files, attributes includes file sizes and cryptographic signatures;

encrypting the client's files utilizing the client's Public Key;

transmitting said encrypted data and file attributes and the client's Public Key signature to said Time Source Provider;

the Time Source Provider creating a TimeMap containing the current time, time source calibration data, file attributes and signatures of any encryption keys used by the client ;

the Time Source Provider returns the client's data along with the time map and session key signature;

the Time Source Provider providing said encrypted client data back to the client; and

the client archives the original files, file attributes and the time map from said Time Source Provider.

2. A method as in claim 1 wherein the client's Public/Private Key pair is organizationally associated.

3. A method as in claim 1, where the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures to the Time Source Provider for inclusion of the time map.

4. A method as in claim 1, further comprising the step of where a session key is exchanged between the client and Time Source Provider for use in generating the signatures of the encrypted files and for securing the transaction.

5. A method as in claim 1 for application of multiple or differing error correcting codes to the representation of the time, the time source calibration data, the file attributes and encryption key signatures.